recipient;

associating the content data with dispatch record data which includes at least said time related indicia and an indicia relating to the destination of the dispatch, to generate authentication data which authenticate the dispatch and the contents of the dispatch; and

securing at least part of the authentication data against tampering of at least the sender.

159. A certificate for attesting a dispatch and contents of the dispatch, comprising a representation of the following authentication data

content data representative of the contents of a dispatch being electronically transmitted by a sender; and

dispatch record data which includes at least an indicia relating to a time of the dispatch and an indicia relating to the destination of the dispatch, said time related indicia being provided in a manner resistant to or indicative of tampering by either of the sender and the recipient, and at least part of said authentication data being secured against tampering of at least the sender.

160. A method for verifying the authenticity of either of the contents, the time and the destination relating to a dispatch from a sender to a recipient, comprising the steps of:

providing a representation of either of said information elements;

verifying said representation for match with a representation of at least part of authentication data, said authentication data comprising a representation of the following information elements: content data representative of the contents of the dispatch being electronically transmitted by the sender, and dispatch record data which includes at least an indicia relating to a time of the dispatch and an indicia relating to the destination of the

dispatch, said time related indicia being provided in a manner resistant to or indicative of tampering by either of the sender and the recipient, and said authentication data being secured against tampering of at least the sender.

161. A method according to claim 160 wherein the step of verifying includes verifying according to a verifiable digital signature verification procedure.

REMARKS

This Amendment adds four claims to particularly point out and distinctively claim the invention. The new claims are all supported by the specification of the corresponding international application as filed and do not add any new (subject) matter to the application.

More particularly, claim 158 is directed to an embodiment where a dispatched document is received electronically (e.g. by fax or e-mail) but sent manually as a printed paper document to the recipient. Support for this claim is found at page 12, lines 12-14 relating to Fig. 1 which illustrates manual delivery of documents:

> ...Alternatively, the documents could be provided to the service via transmission (e.g., by facsimile machine) rather than manually.

Claim 159 is directed to the authentication data generated according to the invention, rather than the process of generating it. Support for this claim is found at page 32, lines 1-12 relating to FIG. 7:

> The service 750 then associates the above data elements for example by generating their fingerprint, which is then signed using the service's private key 752, to produce the service's signature 742. Signing the fingerprint can reduce the resulting signature 742 computation time, transmission bandwidth and storage space. The service then provides back to the sender 701 a service's generated certificate 740 comprising the